دستورات کار با فایل‌ها و فولدرها

این دستورات همون‌هايي هستند که در سيستم‌عامل باستاني!! مايکروسافت يعني MS DOS استفاده مي‌شدند. کاربران ويندوز معمولا نيازي به يادگيري آنها احساس نمي‌کنند چون همه کارها را در محيط گرافيکي و معمولا از طريق ماوس انجام مي‌دهند. ولي چون shell حالت متني دارد، شما بايد با اين دستورات آشنا بشويد. shell را باز کنيد. متن زير ظاهر مي شود:

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

I:\>
```

دقت کنيد که سيستم‌عاملي که من shell را در آن آوردم، ويندوز ۲۰۰۰ است و درايو پيش‌فرض من که معمولا همان درايوي است که ويندوز در آن نصب شده، درايو I است. شما مسلما چيز متفاوتي خواهيد ديد. مي‌نويسم:

```
I:\> C:
```

تا به درايو C وارد بشويم. حالا prompt تغيير مي‌کنه و نشون ميده که الان در درايو C هستم:

```
C:\>
```

مي‌نويسم:

```
C:\> dir
```

و ليست زير ظاهر ميشه:

```
 Volume in drive C is FREE-START
 Volume Serial Number is 3623-07E6

 Directory of C:\

09/06/2003  06:29a    <DIR>          GAMES
08/15/2003  06:20p         1,806,727 phpMyAdmin-2.5.3-rc1-php.zip
06/17/2002  07:06p    <DIR>          upload
```

www.FarazNetwork.ir

```
06/19/2002  07:02p      <DIR>          mail server
09/13/2002  03:59a              8,053 port-tcp-c.c
02/27/2003  10:28p      <DIR>          mp3
04/18/2003  07:38a              1,152 araz.pl
               3 File(s)      1,815,932 bytes
               4 Dir(s)      95,502,336 bytes free
```

اينها در واقع ليست فايل‌ها و دايركتوري‌هاي موجود در درايو C كامپيوتر من است. مثلا اينجا GAMES يک فولدر (دايركتوري) است چون در در اون سطر كلمه <DIR> اومده كه معني دايركتوري ميده. ولي araz.pl كه آخرين سطر از ليسته، فايل هستش حالا مي‌نويسم:

```
C:\> cd games
```

و جواب مي‌شنوم:

```
C:\GAMES>
```

يعني وارد فولدري به اسم games شده‌ام. بازم دستور dir رو مي‌نويسم كه ببينم در اين فولدر چه فايل يا فولدرهايي هست و جواب مي‌شنوم:

```
 Volume in drive C is FREE-START
 Volume Serial Number is 3623-07E6

 Directory of C:\GAMES

09/06/2003  06:29a      <DIR>          .
09/06/2003  06:29a      <DIR>          ..
09/06/2003  06:29a      <DIR>          FORMULA1
09/06/2003  06:35a      <DIR>          SP
09/06/2003  06:36a      <DIR>          SUPER
09/06/2003  06:39a      <DIR>          UF
               0 File(s)              0 bytes
               6 Dir(s)      95,502,336 bytes free
```

www.FarazNetwork.ir

که نشان می دهد ۶ دايركتوري وجود داره. دوتاي اولي دايركتوري‌هاي واقعي نيستند، چون اگه بنويسم:

```
C:\GAMES> cd .
```

جواب مي‌گيرم:

```
C:\GAMES>
```

يعني هيچ اتفاقي نيفتاد. و اگه بنويسم:

```
C:\GAMES> cd ..
```

جواب مي‌شنوم:

```
C:\>
```

يعني يه فولدر به عقب برگشتم و اومدم به همون ريشه درايو C که قبلا بودم. پس الان در درايو C هستم و چون قبلا ديده‌ام که فايلي به اسم araz.pl در اون هست مي‌خوام محتويات اين فايل متني رو ببينم. مي‌نويسم:

```
C:\> type araz.pl
```

و جواب مي‌شنوم:

```
#!/usr/bin/perl
print "Content-type: text/html\n\n";

use Socket;
my ($remote, $port, @thataddr, $that, $them, $proto, $getpage );

$remote = shift || 'www.securitytracker.com';
$port = 80;
@thataddr=gethostbyname($remote) or die "Not Connected";

$that=pack('Sna4x8',AF_INET, $port, $thataddr[4]);
$proto=getprotobyname('tcp');
```

www.FarazNetwork.ir

```
socket(SOCK, PF_INET, SOCK_STREAM, $proto) or die $!;
connect(SOCK, $that) or die $!;
.....
```

اين محتويات فايل araz.pl است. مي‌خوام يک متني فايل جديد بسازم، که محتوياتش فقط يک سطر باشه مثلا salam bar to و نامش هم باشه ali1000.txt براي اين‌کار چند راه وجود داره که دو تاشو مي‌گم:

۱- مي‌تونيد بنويسيد:

C:\> **echo salam bar to > ali1000.txt**

۲- و مي‌توانيد بنويسيد:

C:\> **copy con ali1000.txt**

و enter زده و جمله!! Salam bar to را اونجا تايپ کنيد و وقتي تمام شد، ترکيب: CTRL + Z را فشار بدهيد که فايل تموم بشود.

در هر دو حالت چون ما در درايو C و در ريشه (يعني نه در يک فولدر خاص) بوديم، فايل همين‌جا درست ميشود و اگه دستور dir را اجرا کنيد،مي‌بينيد که يک فايل جديد به ليست اضافه شده. حالا مي‌توانيد با دستور:

C:\> **type ali1000.txt**

محتويات فايل را ببينيد، اگرچه حالا هم مي‌دونيد چي هست! مي‌خواهيم يک فولدر جديد به اسم tur2 بسازيم. مي‌نويسيم:

C:\> **md tur2**

حالا اگر dir را بنويسم، مي‌بينم که فولدر جديد ايجاد شده. حالا مي‌خواهيم برويم به فولدري که ساختم. مي‌نويسم:

C:\> **cd tur2**

و بعد dir مي‌گيرم. مي‌بينم فعلا فقط همان دو فولدر . و .. در اينجا وجود داره که قبلا گفتم چي هستند. اگه بخواهيم يک فولدر جديد در داخل اين فولدر tur2 به اسم far30 بسازم، مي‌نويسم:

C:\tur2> **md far30**

و اگر dir بگيرم، مي‌بينم اينها وجود دارند:

```
 Volume in drive C is FREE-START
```

www.FarazNetwork.ir

```
 Volume Serial Number is 3623-07E6

 Directory of C:\tur2

10/04/2003  07:17p    <DIR>          .
10/04/2003  07:17p    <DIR>          ..
10/04/2003  07:18p    <DIR>          far30
               0 File(s)              0 bytes
               3 Dir(s)      95,477,760 bytes free
```

يعني فولدر far30 هم اضافه شده. مي‌خوام فايل ali1000.txt را از ريشه به فولدر far30 كه خودش در فولدر tur2 است، كپي كنم. مي‌نويسم:

```
C:\tur2> copy c:\ali1000.txt c:\tur2\far30
```

ساختارش خيلي ساده است، حتما فهميدين كه اول دستور copy را مي‌نويسم. بعد با يک فاصله، مسير و نام فايلي كه مي‌خواهيم كپي كنم را مي‌نويسم و در آخر با يک فاصله، مسيري كه مي‌خوام فايل كپي بشود را مي‌نويسم. دقت كنيد كه فايل اصلي دست نخورده باقي مي‌ماند و يک كپي جديد در مسير جديد ايجاد ميشود. مي‌توانستم همين فايل را به درايو D كپي كنيم كه در اين حالت بايد بنويسم:

```
C:\tur2> copy c:\ali1000.txt d:
```

كه فايل به درايو D كپي بشود. حالا يک دستور جديد، مي‌خواهم فايل ali1000.txt را از درايو C پاک كنم، مي‌نويسم:

```
C:\tur2> del c:\ali1000.txt
```

دقت كنيد كه چون من حالا در فولدر tur2 هستم ولي فايلي كه قراره پاک كنم در ريشه است، مسير را بايد بنويسم، ولي اگر فايل همون‌جايي كه من الان هستم بود، مي‌نوشتم:

```
C:\> del ali1000.txt
```

نكته مهم اينه كه وقتي روي كامپيوتر خودم shell را باز كردم، مي‌توانم ببينم كه كجا قرار دارم (با نگاه به پرامت كه مثلا اينجا c:\tur2> بود) خيلي ساده‌است با دستور زير:

```
cd
```

www.FarazNetwork.ir

که جواب میده:

```
c:\tur2
```

چون قبلا فایل ali1000.txt را به فولدر far30 موجود در فولدر tur2 موجود در درایو C کپي کردم، مي‌رویم همونجا مي‌نویسم:

```
C:\> cd c:\tur2\far30
```

اگه dir بگیرم، اینو مي‌بینم:

```
 Volume in drive C is FREE-START
 Volume Serial Number is 3623-07E6

 Directory of C:\tur2\far30

10/04/2003  07:18p    <DIR>          .
10/04/2003  07:18p    <DIR>          ..
10/04/2003  07:08p                15 ali1000.txt
               1 File(s)             15 bytes
               2 Dir(s)      95,477,760 bytes free
```

اگه بخوام این فایل را منتقل کنم به فولدر tur2 از درایو C (یعني به یه فولدر پایین تر) از دستور زیر استفاده مي‌کنم:

```
C:\tur2\far30> move ali1000.txt c:\tur2
```

فرق دستور move با copy اینه که فایل اصلي منتقل میشه نه کپي! یعني از محل قبلي پاک میشود و به محل جدید میاد!! حالا که فولدر far30 خالي شده (یعني هیچ فایل یا فولدري در آن نیست) مي‌توانم پاکش کنم. اول میام یه فولدر پایین‌تر، با دستور:

```
C:\tur2\far30> cd ..
```

و با دستور جدید زیر که مخصوص پاک کردن فولدر (نه فایل) است، فولدر far30 را پاک مي‌کنم:

```
C:\tur2> rd far30
```

و فولدر پاک میشود. حالا مي‌خوام اسم فایل ali1000.txt را به araz.inc تغییر بدهم، مي‌نویسم:

www.FarazNetwork.ir

C:\tur2> **ren ali1000.txt araz.inc**

يه dir بيريد كه مطمئن بشيد!! حالا مي‌خوام يه كپي از اين فايل كه اسمش هست araz.inc بگيرم ولي با اسم ali1000.inc و در همين فولدر. پس مي‌نويسم:

C:\tur2> **copy araz.inc ali1000.inc**

حالا اگه dir بگيريد، ۲ تا فايل مي‌بينيد. حالا مي‌خواهم هر دو تا فايل را منتقل كنم به درايو C ولي به ريشه، مي‌بينم كه هر دو فايل حرف اولشون a است و پسوندشون inc مي‌تونم به دو شكل بنويسم:

C:\tur2> **move a*.inc c:**

ولي چون فقط همين دوتا فايل در اين فولدر بود، مي‌تونستم بنويسم:

C:\tur2> **move *.* c:**

مي‌خواهيم بريم به فولدر و درايوي كه فولدر ويندوز باشد. مي‌توانم يكي يكي درايو ها را بريم و از همه dir بگيرم تا برسم به اوني كه درايو winnt داره، ولي چون اين كامپيوتر خودمه و مي‌دونم كه فولدر ويندوز من كجاست!! مي‌نويسم:

C:\tur2> **I:**

و بعد

I:\> **cd winnt**

و يک dir مي‌گيرم. مي‌بينم كه لسيتي از فايل‌ها و فولدرهاي زيادي از جلو چشم رد ميشه ولي نمي‌تونم همه را ببينم. اگه بخوام صفحه به صفحه ببينم، مي‌نويسم:

I:\winnt> **dir /p**

كه اين سويچ p مخفف page است. اگه بخواهيد ليست همه سويچ‌ها را ببينيد، مي‌توانيد بنويسيد:

I:\winnt> **dir /?**

حالا يه چيز جالب! با دستورات زير اول برگرديم به ريشه درايو I و بعد برگرديم درايو C :

I:\winnt> cd ..

I:\> C:

حالا مي‌خواهم مستقيما از درايو C محتويات فولدر winnt از درايو I را آن هم به صورت صفحه به صفحه بخوانم:

C:\> **dir i:\winnt /p**

www.FarazNetwork.ir

حالا يه چيز بسيار مهم، مي‌خوام بدون دادن مسير! ليست فايل‌ها را در فولدر مربوط به ويندوز ببينم:

```
C:\> dir %SystemRoot%
```

پس در Shell كلمه %SystemRoot% يعني فولدر ويندوز. يه سويچ جديد براي دستور dir را مي‌خوام بگم. فرض كنيد كه من يادم رفته فايل اجرايي cmd.exe در كدام فولدر از درايو I (كه در كامپيوتر من فولدر مربوط به ويندوز هست) قرار داره. چون نمي‌تونم برم تک تک فولدرها را ببينم، بايد از سويچي استفاده كنم كه وقتي يه مسير بهش مي‌دهم، بره و تمام مسير های آن فولدر (يعني همام فولدرهاي داخلي‌تر) را هم ببينيه. از سويچ s استفاده مي‌كنم و مي‌نويسم:

```
C:\> dir i:\cmd.exe /s
```

و جواب مي‌شنوم:

```
 Volume in drive I has no label.
 Volume Serial Number is DC24-A09D

 Directory of i:\WINNT\system32

12/07/1999  04:00a           236,304 cmd.exe
               1 File(s)        236,304 bytes

 Directory of i:\WINNT\system32\dllcache

12/07/1999  04:00a           236,304 cmd.exe
               1 File(s)        236,304 bytes

    Total Files Listed:
               2 File(s)        472,608 bytes
               0 Dir(s)   1,255,153,664 bytes free
```

پس اين دستور توانست فايل مربوطه را در دو تا فولدر پيدا كنه، يعني اينا:

```
i:\WINNT\system32
```

www.FarazNetwork.ir

```
i:\WINNT\system32\dllcache
```

اين cmd.exe همونه كه ما در run نوشتيم كه shell ويندوز اومد. حالا برمي‌گردم به درايو C (دستورش كه يادتون هست!) و dir مي‌گيرم و مي‌بينم كه فايل ali1000.inc هنوز هم اونجا هست. مي‌خوام يه دستور جديد را بگم. ببينيد گاهي پيش مياد كه ما فايلي را به يک سرور مي‌فرستيم ولي مي‌خوايم به صورت مخفي يا hidden باشه. دستوري كه فايل ali1000.inc را مخفي مي‌كنه، اينه:

```
C:\> attrib +h ali1000.inc
```

حالا اگه dir بگيرم، ديگه فايل ali1000.inc را نمي‌بينم. البته هنوز هم هست!! اگه بخواهلم به كمک دستور dir فايل‌هاي مخفي را (از جمله ali1000.inc) ببينم، از سويچ a استفاده مي‌كنيم:

```
C:\> dir ali1000.inc /a
```

حالا مي‌خوام فايل را از حالت مخفي در بيارم، مي‌نويسم:

```
C:\> attrib -h ali1000.inc
```

به همين راحتي!

اينا دستورات معمولي dos بود كه براتون نوشتم. اين دستورات خيلي زياد هستند و من فقط تعداد كمي‌شو براتون گفتم. اگه كتاب داس تو انباري خونتون پيدا كردين، مي‌تونين دستورات بيشتري ياد بگيريد!!!

پسوند فايل‌ها و مفاهيم آنها در ويندوز

در سيستم‌عامل ويندوز پسوندها مفاهيم خاصي دارند.

۱- فايل‌هاي اجرايي پسوند exe يا com يا bat دارند. (فايل‌هاي با پسوند bat رو batch file مي‌گويند كه مجموعه‌اي از دستورات داس را مي‌توانيد در آن بنويسيد كه به ترتيب اجرا بشوند پس مي‌توانيد به كمک دستور type محتوياتش را ببينيد). ولي فايل‌هاي exe و com فايل‌هاي اجرايي هستند كه محتوياتش براتون قابل خوندن نيست ولي قابل اجراست. حالا مي‌خوام يه فايل اجرايي را براتون بيارم كه ببينيد كه در shell چطوري مي‌تونيد فايل اجرايي را اجرا كنيد! مي‌خوام فايل tftp.exe رو اجرا كنم. اول يه dir مي‌گيرم از فولدر %SyestemRoot% و مي‌بينم كه اين فايل در فولدر i:\winnt\system32 قرار داره. حالا مي‌خوام اجراش كنم. به دو طريق مي‌توانم اين كار را انجام بدم، اولي اينكه برويم تو فولدر winnt\system32 و بعد بنويسم:

```
I:\WINNT\system32> tftp.exe
```

يا اينكه مستقيما از هرجايي كه باشم، بنويسم:

www.FarazNetwork.ir

C:\> **i:\winnt\system32\tftp.exe**

و جواب بشنوم:

```
Transfers files to and from a remote computer running the TFTP service.

TFTP [-i] host [GET | PUT] source [destination]

  -i            Specifies binary image transfer mode (also called
                octet). In binary image mode the file is moved
                literally, byte by byte. Use this mode when
                transferring binary files.
  host          Specifies the local or remote host.
  GET           Transfers the file destination on the remote host to
                the file source on the local host.
  PUT           Transfers the file source on the local host to
                the file destination on the remote host.
  source        Specifies the file to transfer.
  destination   Specifies where to transfer the file.
```

permission ها (مجوزها) در NTFS

مجوزها در NTFS 5.0:

۱- No Access : يعني عدم دسترسي.

۲- Read: فقط خواندني. در NTFS 4.0 در حالت Read مي‌تونستيم فايل‌هاي اجرايي داخل آن فولدر را اجرا كنيم ولي در NTFS 5.0 با اين مجوز نمي‌توانيم فايل‌هاي اجرايي را اجرا كنيم و فقط مي‌توانيم بخوانيم.

۳- Execute & Read: يعني اجازه خواندن و نيز اجازه اجرا كردن.

۴- Write: يعني اجازه خواندن، اجرا كردن و تغيير دادن.

www.FarazNetwork.ir

۵- Modify: دقيقا مثل Write + اجازه تغيير

۶- Full Control: يعني مثل Write + اجازه تغيير مجوزها

Share ها در ويندوز سرور

share در ويندوز سرورها يعني منابعي كه از طريق شبكه (يعني از راه دور) قابل دسترسي باشد. دسترسي به منابع اشتراكي در ويندوز سرورها، از طريق پروتكل SMB است كه مايكروسافت آن را CIFS ميگويند. در اين حالت، اول يک احراز هويت داريم و بعد از آن يک session يا نشست تشكيل ميشود (يک چيزي هم به اسم Null Session هست كه توضيحاتش در همان درس اومده.) پروتكل‌هاي قديمي NetBEUI (كه از دور خارج شده) و NetBIOS هم چيزي است هنوز هم توسط ويندوز ساپورت ميشه. منابع اشتراكي هم كه مشخصه: فولدرها، درايوها و چاپگر.

حالا مي‌رسيم به ليست share ها:

IPC$: يعني دسترسي كامل. اگر بتوانيم به اين share برسيم در واقع به تمام فايل‌ها، درايوها و فولدرها دسترسي داريم. معمولا دسترسي به اين share فقط براي اكانت‌هاي Admin است.

**ADMIN$** : اين share مربوط به فولدري است كه ويندوز در آن نصب شده است يعني %SystemRoot% بنابراين share محدودتري نسبت به IPC$ محسوب ميشود.

print$: يعني چاپگر! فولدر مربوطه‌اش اينجاست: %SystemRoot%\system32\spool\PRINTERS يعني با اين share به اين فولدر دسترسي داريم. اين فولدر جايي است كه كارهاي چاپي به صورت فايل‌هايي با پسوند spl نگهداري مي‌شوند.

C$** و **D$ و...: اگه اين share ها ست شده باشه به درايوهاي C و D و ... دسترسي داريم.

share هاي ديگر: هر فولدري را در ويندوز ميشود share كرد و يک نام خاص به آن نسبت داد...

www.FarazNetwork.ir

سایر دستورات خط فرماني در ویندوز سرورها

یک سري دستورات خط فرماني در قسمت اول این مجموعه درس‌ها بررسي شد. بیشتر دستورات خط فرماني که بیان می کنیم ، از مجموعه دستور net ویندوز هستند (یعني با عبارت net شروع مي‌شوند) و اکثرا لازم است که با اکانتي در حد Administrator باشید که اجرا بشوند. یه مطلب دیگر اینکه وقتي مي‌گوییم که یه دستور به صورت لوکال هم مي‌تواند اجرا بشود، روي ویندوز NT کامپیوتر خودتون هم مي‌توانید تست کنید. مطلب بعدي اینکه این دستورات کاربردهاي زیادي دارند ولي ما فقط مواردي را بررسي مي‌کنیم .

۱- **net help** :

این دستور در واقع help دستور net است. مي‌نویسم:

```
net help
```

و جواب مي‌شنوم:

```
The syntax of this command is:


NET HELP command
    -or-
NET command /HELP


  Commands available are:


  NET ACCOUNTS            NET HELP            NET SHARE
  NET COMPUTER            NET HELPMSG         NET START
  NET CONFIG              NET LOCALGROUP      NET STATISTICS
  NET CONFIG SERVER       NET NAME            NET STOP
  NET CONFIG WORKSTATION  NET PAUSE           NET TIME
  NET CONTINUE            NET PRINT           NET USE
  NET FILE                NET SEND            NET USER
```

www.FarazNetwork.ir

```
NET GROUP        NET SESSION        NET VIEW


NET HELP SERVICES lists the network services you can start.

NET HELP SYNTAX explains how to read NET HELP syntax lines.

NET HELP command | MORE displays Help one screen at a time.
```

توضیحات کاملا واضحه. مثلا اگر بخواهیم در مورد دستور net time و کاربردش اطلاعات بگیرم، باید بنویسم:

```
net help time
```

یا

```
net time /help
```

تا توضیحات بیاد.

۲- **net helpmsg**:

وقتي كه يک دستور net به صورتي اجرا ميشود كه خطايي پيش بياد، ويندوز يک شماره خطاي ۴ رقمي به ما ميدهد كه براي دريافت جزئيات بيشتر در مورد اين خطا بايد از دستور net helpmsg استفاده كنيم. مثلا مي‌نويسم!

```
net share shanguli_mangul_habbeye_angur
```

و جواب مياد:

```
This shared resource does not exist.


More help is available by typing NET HELPMSG 2310.
```

يک خطا رو گزارش داده و يک عدد ۴ رقمي به من داده. براي اينكه بدونم جزئيات خطا چيه، مي‌نويسم:

```
net helpmsg 2310
```

و به من بگوييد اشتباه من چه بوده است...

۳- **net time** :

ما از اين دستور براي فهميدن زمان روي يک سرور استفاده مي‌كنيم. اگه به صورت لوكال استفاده مي‌كنيد بنويسيد:

www.FarazNetwork.ir

net time

ولي اگه به صورت remote كار مي‌كنيد (يعني يک session NetBIOS تشكيل داده‌ايد توسط دستور net use كه در درس پورت ۱۳۹ هم توضيح داده شده)، بنويسيد:

**net time **xxx.xxx.xxx.xxx

كه xxx.xxx.xxx.xxx همان ip ي است كه session براش داريم.

۴- **net use** :

اين دستور دو كاربرد مهم داره كه در بحث پورت ۱۳۹ بحث شده‌است. اولين كاربرد connect يا disconnect شدن به يک كامپيوتر با پورت ۱۳۹ باز و NetBIOS فعال است. مثلا اگه بخوام با اكانت Administrator با پسورد yechizi به كامپيوتري با ip ي xxx.xxx.xxx.xxx كانكت بشم به share ي به اسم IPC$ (اين share معمولا هست، به همين دليل از اين share استفاده كردم.) ، مي‌نويسم:

net use **xxx.xxx.xxx.xxx**IPC$ "yechizi" **/user:**"Administrator"

اين كاربرد اول بود كه اين را قبل از دستور net view انجام مي‌دهيم. مي‌توانستيم يک Session null تشكيل بدهيم، به اين صورت كه قسمت مربوط به username و password را خالي بذاريم. به اين صورت:

net use **xxx.xxx.xxx.xxx**IPC$ "" **/user:**""

حالا session تشكيل شده است! كاربرد بعدي اين است كه بعد از اينكه دستور بالا را اجرا كردم و بعد دستور net view را اجرا كردم و ليست كامل share ها را بدست آوردم، بيام و يكي از اين share ها را استفاده كنم. مثلا اگه اسم share كه ليست شده، SharedDocs باشه، و بخوام يک درايو جديد را بهش نسبت بدم كه بتونم باهاش كار كنم، مي‌نويسم:

**net use * **xxx.xxx.xxx.xxx\SharedDocs

معني كاراكتر * اين است كه اگر مثلا آخرين درايو در كامپيوتر من (با احتساب سي-دي درايو) مثلا G باشه، درايوي كه براي share استفاده مي‌شود، درايو بعدي يعني H باشه. مي‌توانستم اينطوري هم بنويسم:

**net use H: **xxx.xxx.xxx.xxx\SharedDocs

www.FarazNetwork.ir

خوب حالا مي‌توانم مثل يک درايو محلي باهاش کار کنم. توي درس پورت ۱۳۹ مي‌اومديم و My Computer را از دسکتاپ باز مي‌کرديم و با درايو جديد کار مي‌کرديم. چون ما دستورات داس را ياد گرفته‌ايم مي‌توانيم با اين دستورات هم با آن درايو کار کنيم، مثلا بنويسيم:

```
H:
dir
,...
```

وقتي کارمون با share تموم شد، بايد disconnect کنيم، با اين دستور :

```
net use /delete H:
```

تا ارتباط قطع بشه.

۵- **net view** :

Netbios session تشکيل داده‌ام (گاهي Null Session هم جواب ميده) و حالا مي‌خوام ببينم که چه منابعي برام share شده، مي‌نويسم:

```
net view \\xxx.xxx.xxx.xxx
```

و مثلا جواب مي‌گيرم:

```
Shared resources at \\xxx.xxx.xxx.xxx

Share name   Type         Used as   Comment

-------------------------------------------
SharedDocs   Disk
The command completed successfully.
```

مي‌بينيد که SharedDocs فولدري‌است که share شده. حالا با دستور net use مي‌تونم از share استفاده کنم.

۶- **share net** :

اين دستور به ما کمک مي‌کنه که share ها را به صورت لوکال مديريت کنيم (دستور بالايي به صورت remote استفاده مي‌شد) . مي‌خوام ببينم که چه share هايي الان هست. مي‌نويسم:

www.FarazNetwork.ir

net share

و جواب مي‌گيرم:

```
Share name   Resource                    Remark

-------------------------------------------------------------------------------
F$           F:\                         Default share
IPC$                                     Remote IPC
D$           D:\                         Default share
I$           I:\                         Default share
G$           G:\                         Default share
E$           E:\                         Default share
ADMIN$       I:\WINNT                    Remote Admin
H$           H:\                         Default share
C$           C:\                         Default share
J$           J:\                         Default share
The command completed successfully.
```

همشون پر واضح‌اند! خوب حالا مي‌خوام مثلا C$ را از ليست share ها پاک کنم. مي‌نويسم:

net share C$ **/delete**

اگه دوباره ليست را بيارم، مي‌بينم که ديگه نيست. مي‌خوام دوباره همون را share کنم، مي‌نويسم:

net share C$=C:

حالا مي‌خوام مثلا فولدر C:\ali را به اسم info بيام و share کنم، مي‌نويسم:

net share info=c:\ali

حالا اگه ليست بگيرم، مي‌بينم که وارد ليست شده.

۷- **net accounts** :

Account Policy را براي اکانتي که با اون وارد شده‌ايم بيان مي‌کند. به‌صورت لوکال استفاده مي‌شود.

مي‌نويسم:

www.FarazNetwork.ir

net accounts

و مثلا جواب مي‌شنوم:

```
Force user logoff how long after time expires?:       Never
Minimum password age (days):                          0
Maximum password age (days):                          42
Minimum password length:                              0
Length of password history maintained:                None
Lockout threshold:                                    Never
Lockout duration (minutes):                           30
Lockout observation window (minutes):                 30
Computer role:                                        SERVER
The command completed successfully.
```

تنها قسمتي كه نياز به توضيح دارد، عبارت Lockout است. اين يک ويژگي امنيتي است. فرض كنيد كه كسي مي‌خواد از طريق امتحان كردن تعداد زيادي پسورد براي يک اكانت، پسورد را پيدا كند . مي‌توانيم جوري اكانت را تنظيم كنيم كه مثلا بعد از سه بار تست ناموفق، به مدت چند دقيقه locak يا قفل بشه.

۸- **net user** :

اين دستور به ما كمک مي‌كنه كه به صورت لوكال بدونيم كه چه اكانت‌هايي در سيستم تعريف شده است و نيز اينكه اطلاعاتي در مورد هريک بدست بياريم و نيز اكانت جديد تعريف كنيم. اول مي‌خوام بدونم چه اكانت‌هايي تعريف شده، مي‌نويسم:

net user

و جواب مي‌شنوم:

```
User accounts for \\computer-name

-------------------------------------------------------------------------------
Administrator            ali                      araz
ASPNET                   Guest
```

www.FarazNetwork.ir

```
The command completed successfully.
```

خوب حالا مثلا مي‌خوام راجع به اكانت guest اطلاعاتي بگيرم، مي‌نويسم:

```
net user guest
```

و جواب مي‌گيرم:

```
User name                    Guest
Full Name
Comment                      Built-in account for guest access to the computer/domain
User's comment
Country code                 000 (System Default)
Account active               No
Account expires              Never

Password last set            10/27/2003 2:58 AM
Password expires             Never
Password changeable          10/27/2003 2:58 AM
Password required            No
User may change password     No

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   Never

Logon hours allowed          All

Local Group Memberships      *Guests
```

www.FarazNetwork.ir

Global Group memberships *None

The command completed successfully.

مي‌بينيد كه در سطر ۲ تا مونده به آخر (سطري Local Group Membership) دقيقا بيان شده كه اين اكانت به چه گروه‌هايي تعلق داره. دقت كنيد كه به‌جاي دستور net user از دستور net users هم مي‌تونيد استفاده كنيد.

حالا مي‌خوام يک اكانت جديد اضافه بكنم. اسم اكانت مي‌خوام vahid باشه و پسورد اون yechizi مي‌نويسم:

net user vahid yechizi **/add**

حالا مي‌خوام همين اكانت را پاک كنم:

net user vahid **/delete**

دقت كنيد كه در دستور پاک كردن ديگه لزومي به وارد كردن پسورد نيست. دستور بعدي به ما ميگويد كه چطوري يک اكانت را وادار كنيم كه عضو يک گروه محلي شود.

۹- **net localgroup** :

ليست گروه‌هاي محلي تعريف شده را بيان مي‌كند و نيز ميشود فهميد در هر كدوم از اين گروه‌ها چه اكانت‌هايي هست ونيز ميشه به يک گروه خاص اكانتي اضافه كرد. مي‌خوام ببينم كه چه گروه‌هاي محلي تعريف شده است. مي‌نويسم:

net localgroup

و جواب مي‌شنوم:

Aliases for *Computer-name*

---

*Administrators *Backup Operators *Debugger Users

*DHCP Administrators *DHCP Users *Guests

*Power Users *Replicator *Users

The command completed successfully.

www.FarazNetwork.ir

دقت کنید که ویندوز معمولا هنگام ارائه نتایج دستورات net میاد و اول اسم هر گروه یک * قرار میده تا با اکانت‌ها اشتباه نشه. حالا مي‌خوام ببینم که مثلا در گروه Administrators چه اکانت‌هايي هست. مي‌نویسم:

```
net localgroup Administrators
```

و جواب مي‌شنوم:

```
Alias name     Administrators

Comment        Administrators have complete and unrestricted access to the computer/domain


Members


-------------------------------------------------------------------------------

Administrator

ali

araz

The command completed successfully.
```

پس سه تا اکانت در حد Admin داریم. حالا مي‌خوام مثلا اکانت ali را از لیست Admin ها خارج کنم، مي‌نویسم:

```
net localgroup Administrators ali /delete
```

و اون اکانت از گروه حذف مي شود (مي‌توانید دوباره لیست بگیرید و ببینید که دیگر در این گروه نیست). حالا مي‌خوام دوباره اکانت ali را به این گروه اضافه کنم، مي‌نویسم:

```
net localgroup Administrators ali /add
```

این دستور از جمله مهم‌ترین دستوراتي است که باید یاد بگیرید. گاهي با اکانتي وارد مي‌شویم و مي‌خواهیم که آن را به حد Admin برسانیم و روش کار همین دستور آخري است وقتي اکانتي وارد گروه Admin میشود، تمام مزاياي همچین گروهي را بدست میاره.

۱۰- **net session** :

به کمک این دستور مشخص میشود که چه کساني الان یک session در سیستم دارند. به عبارت دیگه چه کساني به صورت remote به سیستم وارد شده‌اند. این دستور را تایپ کنید:

www.FarazNetwork.ir

net session

تا ليست اونا بياد. اگه مي‌خوام همه session ها را خاتمه بدم، مي‌نويسم:

net session /delete

اين همه session هاي مرا در كامپيوتري كه درش اين دستور اجرا شده، با ساير كامپيوترها قطع مي‌كند. اگه فقط بخوام يک session را با يه كامپيوتر خاص تموم كنم، مي‌نويسم:

net session **xxx.xxx.xxx.xxx **/delete

اين در حالتي است كه با اون كامپيوتر session داشته باشم. دقت كنيد كه به جاي دستور net session مي‌توانيد از دستور net sessions يا net sess استفاده كنيد.

۱۱- **net send**:

فرض كنيد كه مي‌خوام يک message به فرد خاصي كه الان به سيستم وارد شده و يک session دارد بفرستم. (اينكه فردي session دارد يا نه، به كمک دستور session net قابل بررسي است) بدين منظور از اين دستور مي‌توانم استفاده كنم. مثلا اگه بخوام به Administrator كه الان در سيستم هست، پيغام Salam Refig را بفرستم، مي‌نويسم:

net send Administrator Salam Refig

در اين حالت آن پيغام منو مي‌گيره. اگه بخوام به همه اونايي كه الان session دارند، همين پيغام را بفرستم، مي‌نويسم:

net send /users Salam Refig

و پيغام و همه مي‌گيرند. اين دستور بايد به صورت local يعني از طريق يک shell اجرا بشه.

۱۲- ساير دستورات net :

يک سري دستورات net هستند مثل net computer و net group كه در شبكه‌اي از ويندوز سرورها كاربرد دارند و بعدها بررسي خواهند شد. و نيز يک سري دستور براي مديريت سرويس‌ها داريم مثل net config و net stop و net continue و net pause و start net كه در جلسه بعدی توضیح می دهم.

www.FarazNetwork.ir